클라우드 포렌식을 위한 오픈스택 플랫폼에서 로그데이터 수집†

한수빈*, 이병도*, 심종보** 신상욱**
*부경대학교 대학원 정보보호학(협)
**부경대학교 IT 융합응용공학과
e-mail : subin4853@naver.com

Log Acquisition of the OpenStack Platform for Cloud Forensic

Su bin Han*, Byung-Do Lee*, Jongbo Shim**, Sang Uk Shin**
*Interdisciplinary Program of Information Security, Graduate School, Pukyong National University
**Dept. of IT Convergence and Application Eng, Pukyong National University

요 약

클라우드 컴퓨팅의 많은 장점에도 불구하고 클라우드 컴퓨팅은 보안이슈는 줄어들지 않으며, 특히 디지털 포렌식은 실질적인 기능을 수행하기에 미비한 실정이다. 최근, 다양한 사이버 범죄가 증가하면서 클라우드 컴퓨팅 환경은 사이버 범죄에 노출되어 있으며 악의적인 공격의 위험을 가지고 있다. 클라우드 포렌식은 자원이 가상공간에 존재할 수 있고, 증거 데이터가 물리적으로 분산되어 있기 때문에 기존의 포렌식 수사와는 다르게 접근해야 한다. 또한, 클라우드 기반 포렌식에서 획득 가능한 증거 데이터에 대한 정의가 되어 있지 않아서 증거 데이터를 수집하는데 어려움을 겪는다. 이에 본 논문에서는 오픈스택 플랫폼을 이용한 클라우드 환경을 구축하고, 클라우드 플랫폼 기반 포렌식을 위해 획득 가능한 로그 데이터에 대해 정리하고, 실제 획득 가능한 로그를 수집 및 분석하고, 클라우드 컴퓨팅 플랫폼기반 포렌식의 한계점과 해결방안을 알아본다.

1. 서론

최근 IT 기술의 발전과 함께 사이버 범죄가 증가하면서, 다양한 사이버 범죄 사례가 늘어나고 있는 추세이다. 이러한 사이버 범죄에서 클라우드 컴퓨팅은 사이버 범죄의 새로운 타깃이 되고 있다. 클라우드 컴퓨팅은 이미 국내외 기업뿐만 아니라 일반 개인 사용자들에게도 많은 관심을 받고 있지만, 클라우드 컴퓨팅 시장의 급격한 성장에도 불구하고 클라우드 컴퓨팅에 대한 디지털 포렌식은 새로운 기술 및 법적 문제를 발생시키고 있다[6]. 클라우드 컴퓨팅은 증거를 수집할 때, 물리적인 액세스의 부족과 원격이라는 특성을 가지기 때문에 기존의 포렌식 수사와 다르게 접근해야 하지만 이에 해당하는 포렌식 도구, 실질적인 정책 등에 관한 연구가 미비한 실정이다. 이에 따라 성장하는 클라우드 컴퓨팅 시장과 사이버 범죄에 대응하여 클라우드 컴퓨팅에 대한 이해를 바탕으로 디지털 포렌식 시스템을 체계적으로 준비할 필요가 있다[7].

또한, 클라우드 컴퓨팅에서 디지털 포렌식 조사를 수행 할 때 클라우드 컴퓨팅 특징을 고려한 조사가 요구된다. 클라우드 컴퓨팅은 자원이 가상공간에 존재하거나, 증거 데이터가 물리적으로 분산되어 있기 때문에 일반적인 디지털 포렌식 조사 수행이 어려우며, 클라우드 기반 포렌식의 증거 데이터에 대한 정의가 되어 있지 않고, 클라우드 기반 포렌식 도구가 부족하기 때문에 증거수집 및 분석에 어려움을 겪는다[6].

따라서, 이 논문에서는 가상화된 자원들을 서비스 목적에 따라 폭넓게 활용할 수 있도록 관리 체계를 제공해 주는 클라우드 플랫폼을 기반으로 증거 데이터를 획득 하기 위해, 먼저 일반적인 디지털 포렌식을 대신하여 클라우드 기반 포렌식의 단계를 살펴보고, 실제 클라우드 플랫폼 중에 하나로써 오픈스택을 이용하여 클라우드 환경을 구축하고, 계층에 따른 획득 가능한 증거데이터를 분석하고, 획득 가능한 증거데이터 중에 실제로 로그를 수집하고 수집한 로그에 대해 분석한다.

2. 관련연구

2.1 클라우드 포렌식

J. Dykstra and A. T. Sherman(2013)[1]는 오픈스택 클라우드 컴퓨팅 플랫폼에 대한 디지털 포렌식 도구를 구현했다. 이 논문에 따르면 저자는 도구는 게스트 가

† 이 논문은 2011 년도 정부(미래창조과학부)의 재원으로 한국연구재단-차세대정보컴퓨팅기술개발사업의 지원을 받아 수행된 연구임(No. 2011-0029927).

상 머신 (VM) 또는 하이퍼바이저를 신뢰 할 필요 없이 클라우드 공급자의 지원을 필요로 하지 않고 포렌식 데이터에 대한 액세스를 제공하기 때문에 관리 면에서 사용자 중심의 포렌식 기능을 위한 솔루션이라고 말한다. 그러나 클라우드에 있는 데이터의 보존과 오픈스택의 업데이트에 따른 문제와 같은 문제점을 가지고 있다.

T. Rubsamen and C. Reich(2013)[2]는 클라우드 컴퓨팅 서비스에서 취득할 수 있는 증거를 획득하는 방법과 함께 로깅과 증거를 획득하는 것에 초점을 맞추고 있다.

S. Zawoad and R. Hasan(2013)[3] 는 디지털 포렌식의 수사 과정(그림 1)에 대해 설명하면서 클라우드 포렌식에 대한 전체적인 개요를 명시하면서 클라우드 환경에서 CSP(Cloud Service Provider: 클라우드 서비스 제공자)에 대한 의존도가 높을수록 포렌식 증거를 획득하는데 어렵다는 점과 일반적인 디지털 포렌식과는 다르게 접근해야 한다고 설명하고 있었다. 해결방안으로는 CSP 에 대한 의존도를 줄이고, 보안과 신뢰성을 고려한 포렌식 모델을 구축해야 한다고 언급했다. CSP 의 의존도를 줄이기 위해 오픈스택 계층에서 증거를 획득하려는 점은 같지만, 독립적인 모델을 구축하는 방안이 IaaS 를 제공하는 클라우드 플랫폼에서 증거를 수집하고 획득함으로써 신뢰성과 CSP 의존도를 줄이려는 이 논문의 방향과 다르다. 이 외에도 클라우드 환경에서의 신뢰성 확보[4]와 클라우드 컴퓨팅 환경의 신뢰성 증가를 위한 보안 로깅[5]에 관하여 많은 연구자들이 언급하고 있었다.

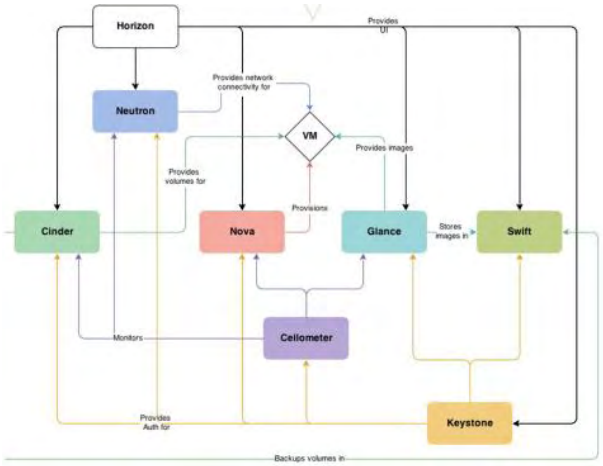
이전의 연구(2014)[7]에서 클라우드 환경에 유연하게 적용 할 수 있는 디지털 증거 수집 절차를 위해, 클라우드 컴퓨팅 시스템 구성 요소의 추상화된 계층에 따른 역할과 수집 가능한 데이터에 대해 분석하였다. 또한, 확보한 증거 데이터의 신뢰성 보장을 위해 클라우드 컴퓨팅 플랫폼 기반의 증거 수집 절차를 제안 하였다.

2.2 오픈소스 클라우드 플랫폼

클라우드 플랫폼은 클라우드를 구축하기 위한 소프트웨어로 서버, 스토리지, 네트워크와 같은 자원들을 수집, 제어, 운영하기 위한 클라우드 운영체제이다. 오픈 소스 소프트웨어로는 오픈스택(OpenStack), 클라우드스택 (CloudStack), 유칼립투스 (Eucalyptus), 오픈네뷸라 (Open Nebula) 등이 있다.

오픈스택은 Rackspace 사와 NASA 의 합작으로 시작된 IaaS(Infrastructure as a Service) 클라우드 플랫폼 프로젝트이다. 이 프로젝트의 목표는 하드웨어에 구애받지 않고 실행되는 클라우드 서비스를 제공하는 것이다[8]. 오픈스택의 구성요소는 개별적인 프로젝트로 명명되어 개발이 진행된다. 그림 1 은 오픈스택 공식 홈페이지에 설치 가이드에서 제공하는 IceHouse 버전의 전체적인 구조를 도식화 한 것이다[9]. 그림 1 에서는 각 프로젝트의 이름과 함께 간단하게 전체적인 흐름을 같이 보여준다. 오픈스택의 대표적인 프로젝트로는 인스턴스의 생명주기를 관리하는 OpenStack Compute(Nova), 정형화되지 않은 데이터 객체를 저장하고 조회하는 Object Storage(Swift), 가상머신 디스크를 저장하고 조회하는 Image Service(Glance), 보안인증을 담당하는 Identity(Keystone), 사용자 인터페이스 서비스를 제공하는 Dashboard(Horizen), 네트워크 연결을 가능하게 하는 Netwoking(Neutron)이 있으며, 이 외에도 다양한 프로젝트들이 오픈스택의 구성요소로써 개발 중이다[9].

따라서, 우리는 오픈소스 클라우드 플랫폼 중에서 오픈스택에 대한 이해를 바탕으로 클라우드 기반 포렌식을 위한 클라우드 환경을 구축하고, 클라우드 플랫폼 분석과 수집 가능한 로그들을 정리한다. 이를 바탕으로, 오픈스택에서 실제 획득 가능한 로그를 수집하고 수집한 로그를 분석하고, 분석한 내용을 기반으로 클라우드 플랫폼 기반 디지털 포렌식의 한계와 해결방안에 대해 설명한다.

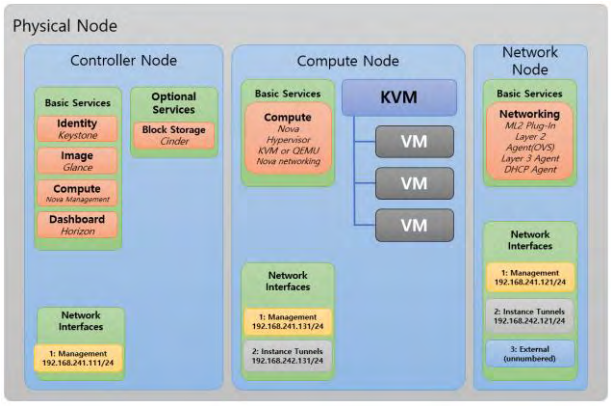


(그림 1) 오픈스택 IceHouse 구조

3. 오픈스택 구축 및 로그 데이터 증거 수집

3.1 오픈스택을 이용한 IaaS 클라우드 환경 구축

오픈스택을 이용한 클라우드 환경을 구축하기 위한 구성은 다양한 방법으로 구성할 수 있다. 이 논문에서는 오픈스택 공식 홈페이지를 참고하여, 3 대의 노드를 이용하여 구축하였다. 그림 2 는 로그 수집을 위해 실제 구축한 환경을 각 노드 별로 설치된 오픈스택 프로젝트와 함께 이해하기 쉽도록 도식화 하였다.



(그림 2) 구축한 오픈스택 노드 구성

먼저, Controller Node 는 플랫폼 전체를 제어하는 역할과 인스턴스의 생명주기를 관리하는 Nova, 오픈스택의 서비스를 위한 인증과 권한부여를 제공하는 Keystone, 웹 기반 사용자 인터페이스를 제공하는 Horizon, 가상 디스크 이미지를 위한 저장소와 목록을 제공하는 Glance, 인스턴스에 영구적인 블록 저장소를 제공하는 Cinder 기능들이 수행된다. Compute Node 는 다수로 구성될 수 있으며 서버 가상화 기능을 제공하는 Xen, KVM 과 같은 하이퍼바이저들이 설치 되어 인스턴스들이 생성되어 실제로 수행되는 물리 서버들이다. 다수로 구성될 경우 마이그레이션이 수행 될 수 있다. 마지막으로, Network Node 는 오픈스택 내부의 가상 네트워크의 구성과 네트워크 서비스를 제공한다[9].

3.2 오픈스택 환경에서의 로그데이터 수집 및 분석

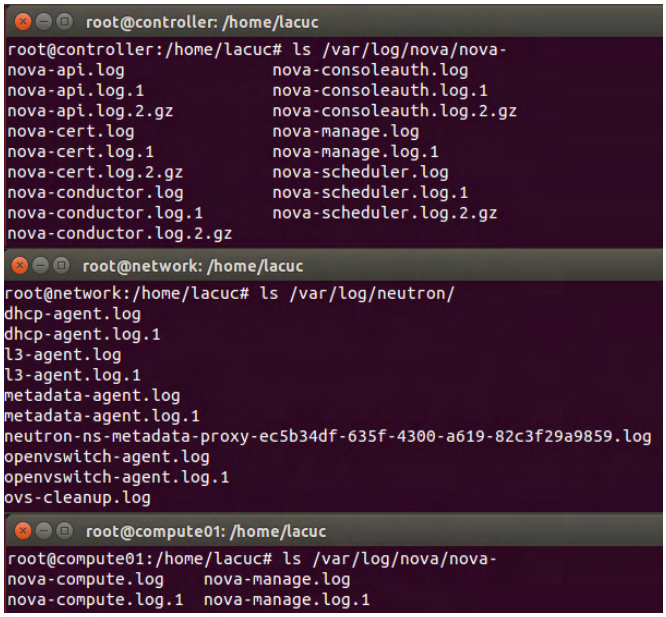
표 1 에서는 오픈스택 환경에서 로그데이터 수집 전에 클라우드 컴퓨팅 시스템 구성 요소의 추상화된 계층에 따른 수집 가능한 로그들을 분류하고 각 계층에 따른 로그들의 위치를 정리 하였다. 수집 이전에 로그 위치와 클라우드 계층에 따른 획득 정보를 정리함으로써, 로그수집을 더 용이하게 한다. 이 논문에서는 오픈스택 기반의 로그 데이터 수집을 수행하므로, Host OS 에서의 로그위치에 따른 수집이 수행된다.

<표 1> 클라우드 컴퓨팅 플랫폼 기반 수집 가능한 로그

Cloud Layer	로그 위치	획득 정보
Guest application	로깅 지원시, 해당 프로그램에 따름	어플리케이션 로그
Guest OS	윈도우: 레지스트리 리눅스: /var/log/*	Guest OS 시스템 이벤트
Hypervisor	qemu : /var/log/libvirt/qemu/ /var/log/libvirt/libvirtd.log	Hypervisor 운영로그 및 생성 인스턴스 로그
Host OS	/var/log/nova /var/log/glance /var/log/cinder /var/log/keystone /var/log/apache2/ /var/log/syslog /var/log/cinder/cinder-volume.log /var/log/neutron	오픈스택의 각 프로젝트 로그
Hardware	/var/log/dmesg	인식되는 하드웨어 정보 로그

오픈스택 각 프로젝트에서 수집 가능한 여러 로그들 중 다음 일부 프로젝트의 로그를 수집하였으며, 각 로그는 다음 정보를 보유하고 있다. 그림 3 은 로그 수집을 위해 구축한 오픈스택에서 각 노드 별 로그 종류를 보여준다. 아래는 그림에서 보여준 Controller, Network, Compute 노드에서 생성되는 로그에 대한 설명이다.

- Controller: 오픈스택과 사용자와의 상호작용과 오픈스택의 다른 구성요소와의 상호작용 메시지 항목을 포함하는 nova-api.log*, 노바 콘솔 서비스와 관련된 인증 세부 정보를 포함하는 nova-consoleauth.log*, nova-cert 프로세스에 관한 메시지 항목을 포함하는 nova-cert.log*, 노바 관리 명령어가 수행될 때의 메시지 항목을 포함하는 nova-manage.log*, 데이터베이스 정보에 대한 요청을 서비스에 대한 메시지 항목을 포함하는 nova-conductor.log*, 큐 공간에서 노드 작업 할당, 메시지, 일정에 관한 항목을 포함하는 nova-scheduler.log*가 있다[10].
- Network: DHCP 에이전트에 관한 로그 항목 포함하는 dhcp-agent.log*, l3 에이전트와 그 기능에 관한 메시지 항목을 포함하는 l3-agent.log*, 노바 메타 데이터 서비스의 프록시인 뉴트론에 관련된 메시지 항목을 포함하는 metadata-agent.log*, open vswitch 작업에 관련된 메시지 항목을 포함하는 openvswitch-agent.log*, 가상 브릿지 br-int 와 br-ex 의 클린업 정보를 포함하는 ovs-cleanup.log*가 있다.[10]
- Compute: compute 노드의 리소스를 추적하고 해당 노드에서 생성되는 인스턴스의 정보를 포함하는 nova-compute.log*, 노바 관리 명령어가 수행될 때의 메시지 항목을 포함하는 nova-manage.log*가 있다.[10]



(그림 3) 노드에 따른 수집되는 로그 종류

수집되는 로그들은 오픈스택 프로젝트의 운용에 관한 정보들이며, 클라우드 플랫폼에서의 오류 또는 각 프로젝트 간의 연결에 대한 정보를 파악 할 수 있다. 이러한 로그정보는 실제 클라우드 포렌식에서 IaaS 를 제공하는 CSP 의 운용 정보를 파악 할 때 사용하거나, 인스턴스의 생성여부 정도만 알 수 있다.

4. 오픈스택 플랫폼 기반 포렌식의 한계 및 해결방안

클라우드 포렌식에서 가장 큰 취약점은 CSP 의 의존성과 대부분의 CSPs 의 포렌식에 대한 인식 부족이다. 이러한 취약점을 해결하기 위해 클라우드 플랫폼 계층에서 포렌식 증거를 획득하고 저장해야 한다. 이러한 방법은 CSP 에 대한 의존도를 줄이고, 증거 데이터의 신뢰성을 높여준다.

그러나, 오픈스택에서 획득한 로그 정보는 해당 프로젝트의 전반적인 운용에 관한 정보이며, 이러한 정보만으로는 최종 사용자가 게스트 OS 상에서 실행한 행위, 인스턴스 내부의 데이터에 대한 정보를 파악하기 어렵다. 또한, 물리적으로 분산된 노드에서 로그를 수집하고, 분석하는 것은 많은 시간과 비용이 발생한다. 따라서, 중앙로그관리를 통해 로그의 신뢰성과 효율성을 높이고, 사용자 이벤트 로그 및 서비스들을 수집하고 분석하기 위해서는 오픈스택 계층에서 인스턴스의 스냅샷 생성 및 보존을 통해 스냅샷의 무결성과 신뢰성을 유지할 수 있는 환경을 구축해야 한다.

5. 결론 및 향후 연구

본 논문에서는 디지털 포렌식을 위해 클라우드 플랫폼기반 로그 데이터를 분류하고, 실제 오픈스택을 구축하여 획득 가능한 로그데이터를 수집하고 분석하는 과정을 수행했다.

그러나, 오픈스택 기반의 로그데이터 획득은 오픈스택의 운영 계층 수준의 로그 내용까지만 파악할 수 있으며, 분산된 환경으로 수집에 따른 비용 및 관리적인 어려움이 있다. 또한, 인스턴스 내에서 실행되는 행위에 대한 분석과 어플리케이션 계층의 로그 정보는 오픈스택에서 제공하는 로그로는 한계가 있다. 이러한 점들을 해결하기 위해 중앙로그관리와 인스턴스의 스냅샷을 제공해주는 포렌식 환경을 구축하기 위해 중앙로그수집과 스냅샷 보존 및 관리에 관한 연구를 예정이다.

참고문헌

[1] J. Dykstra , A .T. Sherman, “Design and implementation of FROST: Digital forensic tools for the OpenStack cloud computing platform”, *Digital Investigation*, Vol 9, pp.87–95, 2013.

[2] T. Rubsamen1, C. Reich, “Evidence for Accountable Cloud Computing Services”, *Pre-Proceedings of International Workshop on Trustworthiness*, Accountability and Forensics in the Cloud (TAFC), 2013.

[3] S. Zawoad, R. Hasan, “Digital Forensics in the Cloud”, *The Journal of Defense Software Engineering*, Vol 26, No.5, pp.17-20, 2013.

[4] I. M. Abbadi, J. Lyle, “Challenges for Provenance in Cloud Computing”, *3rd USENIX Workshop on the Theory and Practice of Provenance*, USENIX Association, 2011.

[5] M. M. Potey, D. D. Nikumbh, “Achieving Accountability and Secure Logging to Increase Trust in Cloud Environment”, *International Journal of Computer Applications*, Vol 73, No.17, 2013.

[6] 이상진, “디지털 포렌식 개론”, 이룬, pp.105-137, 2010.

[7] 한수빈, 이태림, 신상욱, “클라우드 컴퓨팅 디지털 증거 수집 절차”, 정보처리학회 학술발표대회 논문집, Vol 21, No.1, 2014

[8] 김병식, 이범철,"오픈스택을 이용한 클라우드 서비스 플랫폼 구축 및 활용", 한국통신학회 학술대회논문집, 669-670, 2014

[9] www.openstack.org, OpenStack Open Source Cloud Computing Software.

[10] K.Jackson, C.Bunch, "OpenStack Cloud Computing Cookbook Second Edition", Packt Publishing Ltd, 304-306, 2013